WHAT IS CLAIMED IS:

1. A certificate validity authentication method wherein validity of a public key certificate issued by a certification authority which is different from a certification authority trusted by a terminal is authenticated in compliance with a request made by the terminal, comprising:

the path search step of executing a process in which, with any certification authority set as a start certification authority, an issue destination of a public key certificate issued by the start certification authority is checked, and subject to any certification authority included as the issue destination, an issue destination of a public key certificate issued by the issue-destination certification authority is further checked, the process being continued until all of the issue destinations of the public key certificates become terminals, thereby to search for paths which extend from said start certification authority to terminal admitting certification authorities having issued public key certificates to any terminals;

the path verification step of executing for each of the paths detected by said path search step, a process in which, with said start certification authority set at an upstream side, a signature of the public key certificate issued by the terminal admitting certification authority on the pertinent path is verified in the light of the public key certificate issued by the certification authority located directly upstream, and subject

to the verification having held good, a signature of the public key certificate issued by the terminal admitting certification authority located directly upstream is verified in the light of the public key certificate issued by the certification authority located directly upstream still further, the process being continued until said certification authority located directly upstream becomes said start certification authority, thereby to verify said paths;

the path registration step of registering in a database those of said paths whose verifications have held good by said path verification step; and

the validity authentication step of complying with the request of the terminal for authenticating the validity of the public key certificate issued by the terminal admitting certification authority which is different from the certification authority trusted by said terminal, to judge said validity of said public key certificate as having been authenticated when the path between said certification authority trusted by said terminal and said start certification authority and the path between the different terminal admitting certification authority and said start certification authority are held registered in the database.

2. A certificate validity authentication method according to Claim 1, wherein:

said path search step is performed periodically;

said path verification step is performed for a newest path searched for by said path search step; and

said path registration step updates registered contents of said

database to the newest path whose verification has held good by said path verification step.

3. A certificate validity authentication method according to Claim 1, further comprising:

the validity term examination step of examining for each of said paths registered in said database by said path registration step, validity terms of the public key certificates which the certification authorities on the pertinent path have issued to the certification authorities located directly downstream (to the terminals admitted by the terminal admitting certification authorities in a case where the issue origins are said terminal admitting certification authorities); and

the path re-verification step of obtaining any new public key certificate for an issue destination of the public key certificate whose validity term has been authenticated to have expired by said validity term examination step, from the issue origin of the term-expired public key certificate, and verifying at least a signature of the new public key certificate in the light of the public key certificate which has been issued by the certification authority located directly upstream of said issue origin;

wherein said path registration step deletes from said database the path including said issue origin and said issue destination of said public key certificate whose validity term has been authenticated to have expired by said validity term examination step, in either of a case where the verification of the signature of said new public key certificate has not held good at said path re-verification step and a case where said new public

key certificate has failed to be obtained.

4. A certificate validity authentication method according to Claim 1, further comprising:

the revocation information examination step of examining for each of said paths registered in said database by said path registration step, revocation information of the public key certificates which the certification authorities on the pertinent path have issued;

wherein said path registration step deletes from said database the path including said issue origin and said issue destination of any public key certificate which has been authenticated to have been revoked by said revocation information examination step.

5. A certificate validity authentication method according to Claim 1, wherein:

said validity authentication step complies with said request of said terminal for authenticating said validity of said public key certificate issued by said terminal admitting certification authority which is different from said certification authority trusted by said terminal, to judge said validity of said public key certificate as having failed to be authenticated in a case where a constraint to the effect that any certification authority located on said path between said certification authority trusted by said terminal and said start certification authority and said path between said different terminal admitting certification authority and said start certification authority is not trusted, is described in the public key certificate which any certification authority on the two paths has issued to

the certification authority located directly downstream (to the terminal admitted by the terminal admitting certification authority in a case where the issue origin is said terminal admitting certification authority) on the path where the issue-origin certification authority is located, even when said two paths are held registered in said database.

6. A certificate validity authentication method according to Claim 1, wherein:

said validity authentication step complies with said request of said terminal for authenticating said validity of said public key certificate issued by said terminal admitting certification authority which is different from said certification authority trusted by said terminal, to judge said validity of said public key certificate as having failed to be authenticated in a case where the total number of certification authorities located on said path between said certification authority trusted by said terminal and said start certification authority and said path between said different terminal admitting certification authority and said start certification authority exceeds a path length (the maximum allowable number of certification authorities located on the two paths) described in the public key certificate which any certification authority on said two paths has issued to the certification authority located directly downstream (to the terminal admitted by the terminal admitting certification authority in a case where the issue origin is said terminal admitting certification authority) on the path where the issue-origin certification authority is located, even when said two paths are held registered in said database.

7. A certificate validity authentication method according to Claim 1, wherein:

said validity authentication step complies with said request of said terminal for authenticating said validity of said public key certificate issued by said terminal admitting certification authority which is different from said certification authority trusted by said terminal, said request accompanying presentation of trustworthiness required of an electronic procedure intended by said terminal, to judge said validity of said public key certificate as having failed to be authenticated in a case where trustworthiness (policy) described in the public key certificate which any certification authority located on said path between said certification authority trusted by said terminal and said start certification authority and said path between said different terminal admitting certification authority and said start certification authority has issued to the certification authority located directly downstream (to the terminal admitted by the terminal admitting certification authority in a case where the issue origin is said terminal admitting certification authority) on the path where the issue-origin certification authority is located is lower than the trustworthiness required of the electronic procedure, even when the two paths are held registered in said database.

8. A certificate validity authentication method according to Claim 1, wherein said start certification authority is a bridge certification authority which performs cross-certification with respective root certification authorities of at least two security domains.

9. A certificate validity authentication apparatus wherein validity of a public key certificate issued by a certification authority which is different from a certification authority trusted by a terminal is authenticated in compliance with a request made by the terminal, comprising:

path search means for executing a process in which, with any certification authority set as a start certification authority, an issue destination of a public key certificate issued by the start certification authority is checked, and subject to any certification authority included as the issue destination, an issue destination of a public key certificate issued by the issue-destination certification authority is further checked, the process being continued until all of the issue destinations of the public key certificates become terminals, thereby to search for paths which extend from said start certification authority to terminal admitting certification authorities having issued public key certificates to any terminals;

path verification means for executing for each of the paths detected by said path search means, a process in which, with said start certification authority set at an upstream side, a signature of the public key certificate issued by the terminal admitting certification authority on the pertinent path is verified in the light of the public key certificate issued by the certification authority located directly upstream, and subject to the verification having held good, a signature of the public key certificate issued by the terminal admitting certification authority located directly upstream is verified in the light of the public key certificate issued by the certification authority located directly upstream still further,

the process being continued until said certification authority located directly upstream becomes said start certification authority, thereby to verify said paths;

path registration means for registering in a database those of said paths whose verifications have held good by said path verification means; and

validity authentication means complying with the request of the terminal for authenticating the validity of the public key certificate issued by the terminal admitting certification authority which is different from the certification authority trusted by said terminal, to judge said validity of said public key certificate as having been authenticated when the path between said certification authority trusted by said terminal and said start certification authority and the path between the different terminal admitting certification authority and said start certification authority are held registered in the database.

10. A storage medium which stores therein a program for authenticating validity of a public key certificate issued by a certification authority different from a certification authority trusted by a terminal, in compliance with a request made by the terminal;

the program being read and run by an electronic computer, thereby to build on the electronic computer:

path search means for executing a process in which, with any certification authority set as a start certification authority, an issue destination of a public key certificate issued by the start certification authority is checked, and subject to any certification authority included as

the issue destination, an issue destination of a public key certificate issued by the issue-destination certification authority is further checked, the process being continued until all of the issue destinations of the public key certificates become terminals, thereby to search for paths which extend from said start certification authority to terminal admitting certification authorities having issued public key certificates to any terminals;

path verification means for executing for each of the paths detected by said path search means, a process in which, with said start certification authority set at an upstream side, a signature of the public key certificate issued by the terminal admitting certification authority on the pertinent path is verified in the light of the public key certificate issued by the certification authority located directly upstream, and subject to the verification having held good, a signature of the public key certificate issued by the terminal admitting certification authority located directly upstream is verified in the light of the public key certificate issued by the certification authority located directly upstream still further, the process being continued until said certification authority located directly upstream becomes said start certification authority, thereby to verify said paths;

path registration means for registering in a database those of said paths whose verifications have held good by said path verification means; and

validity authentication means complying with the request of the terminal for authenticating the validity of the public key certificate issued by the terminal admitting certification authority which is different from

the certification authority trusted by said terminal, to judge said validity of said public key certificate as having been authenticated when the path between said certification authority trusted by said terminal and said start certification authority and the path between the different terminal admitting certification authority and said start certification authority are held registered in the database.

EP 0 774 860 A1